WYC:lmp 9/26/05 P0376L

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:
Rhoads et al.

Application No.: 09/858,189

Filed: May 14, 2001

For: CONTENT IDENTIFIERS TRIGGERING CORRESPONDING RESPONSES

Examiner: Song, Hosuk

Date: September 26, 2005

Art Unit 2135

Confirmation No. 9322

CERTIFICATE OF MAILING

I hereby certify that this paper and the documents referred to as being attached or enclosed herewith are being deposited with the United States Postal Service on September 26, 2005 as First Class Mail in an envelope addressed to: Mail Stop Appeal Brief – Patents, COMMISSIONER FOR PATENTS, P.O. Box 1450, Alexandria, VA 22313-1450.

William Y. Conwell
Attorney for Applicant

TRANSMITTAL LETTER

MAIL STOP APPEAL BRIEF – PATENTS
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Enclosed for filing in the above-captioned matter are the following:

☒ Appeal Brief (fee **$500.00**)

☒ If any extension of time is required, please consider this a petition therefor.

☒ Please charge **$500.00** (fee for Appeal Brief) and any additional fees which may be required in connection with filing this document and any extension of time fee, or credit any overpayment, to Deposit Account No. 50-3284.

Respectfully submitted,

Date: September 26, 2005

DIGIMARC CORPORATION

CUSTOMER NUMBER 23735

By_____
William Y. Conwell
Registration No. 31,943

Phone: 503-469-4800
FAX 503-469-4777

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:
Rhoads et al.

Application No.: 09/858,189

Filed: May 14, 2001

For: CONTENT IDENTIFIERS TRIGGERING CORRESPONDING RESPONSES

Examiner: Song, Hosuk

Date: September 26, 2005

Art Unit 2135

Confirmation No. 9322

CERTIFICATE OF MAILING

I hereby certify that this paper and the documents referred to as being attached or enclosed herewith are being deposited with the United States Postal Service on September 26, 2005 as First Class Mail in an envelope addressed to: Mail Stop Appeal Brief – Patents, COMMISSIONER FOR PATENTS, P.O. Box 1450, Alexandria, VA 22313-1450.

William Y. Conwell
Attorney for Applicant

Mail Stop: Appeal Brief – Patents
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

This brief is in furtherance of the Notice of Appeal filed July 25, 2005. Please charge the fee required under 37 CFR 1.17(f), or any deficiency, to deposit account 50-3284 (see transmittal letter).

09/29/2005 SDENBOB1 00000007 503284 09858189
01 FC:1402 500.00 DA

I. REAL PARTY IN INTEREST

The real party in interest is Digimarc Corporation, by an assignment from the inventors recorded at Reel 12185, Frames 16-17, on September 20, 2001.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF CLAIMS

Claims 1-14 stand finally rejected and are appealed.

IV. STATUS OF AMENDMENTS

All earlier-filed amendments have been entered.

V. BACKGROUND AND SUMMARY OF CLAIMED SUBJECT MATTER

The present invention concerns techniques for reliably (e.g., redundantly) identifying unknown digital content.

Increasingly, there is a need for technology that identifies music and other digital content, so that systems which encounter such content can treat it appropriately. (A system may respond differently, e.g., to a copyrighted song than to a public domain work.)

One identification technology for digital content goes by the general name of fingerprinting. Many particular implementations are known,[1] but they typically work by processing certain attributes of the content to derive a substantially unique identifier ("UID") that corresponds to the content. This UID serves as the content's "fingerprint."

---

[1] *See, e.g.*, published specification US 2002/0032864, paras. 9-26. (The specification as originally filed was

Another identification technology goes by the general name of digital watermarking. Such technology involves making subtle changes to the digital content (e.g., slightly altering certain sample values) to thereby encode a hidden plural bit message.[2] A content identifier can be hidden in content by such techniques.

(In the case of a watermark, the content identifier can be arbitrarily assigned. In the case of a fingerprint, the content identifier is dependent on the content.)

When a system (e.g., an MP3 player; a TiVo box; a peer-to-peer network, etc.) seeks to identify an unknown piece of content, it must perform a substantial amount of processing to obtain the identifier. In the case of a fingerprint, the system may have to apply a complex mathematical algorithm to compute a fingerprint from the data samples of which the content is comprised. In the case of a watermark, the system must apply a decoding algorithm to the content data to discern the content identifier hidden therein.

To speed such operations, the content identifier can be included as header data that accompanies the content.[3] As is familiar to artisans, content data - such as audio and video – is commonly stored in file data structures that include header fields in which auxiliary information (e.g., title of the work, copyright owner, publisher, etc.) can be conveyed.[4] The distributor of the content file can insert in the header data a content identifier derived from the content by fingerprinting, or encoded in the content by watermarking.

By such arrangements, a system can obtain a fingerprint (for example) from a file in two different ways: (a) by reading it from the header info, or (b) by computing it from the content information. This redundancy offers several advantages. For example, it aids security. If a file has header-stored fingerprint that does not match a fingerprint derived from the file contents, something is amiss – the file may be destructive (e.g., a pernicious Trojan Horse file), or the file structure may mis-identify the contents.[5]

---

not printed with line numbering – thus the reference to the published specification instead.

[2] Various particular watermarking techniques are detailed in documents incorporated-by-reference into the present specification. *See, e.g.,* published specification US 2002/0032864, paras. 1-4 and 38.

[3] *See, e.g.,* published specification US 2002/0032864, para. 29.

[4] *Ibid.*

[5] *Ibid.*

When a system encounters a content file, it can look first in the accompanying header data for a content identifier. Only if the header data doesn't include a content identifier, or if it is suspect, does the system undertake the more complex operation of calculating/decoding the content identifier from the content itself. (The content identifier may be "suspect," e.g., if it doesn't follow a prescribed format, if it fails authentication using digital signature technology, etc.)[6]

Thus, the header data can be the primary source of the content identifier (fingerprint or watermark), with the file contents being processed to re-derive the identifier only if some check of identifier data stored in the header fails.[7]

In some embodiments, the header data may not include the content identifier *per se,* but rather include an electronic address or pointer data indicating another location (e.g., a URL or database record) at which the content identifier is stored.[8]

Once the content identifier is discerned, it can be passed to a database that may respond, e.g., with information providing rules for use of that content.

The present patent application includes two independent claims (1 and 8), generally parallel in structure, but one focused on fingerprint technology, and the other on watermark technology. (None of the claims has been amended during prosecution.) Claim 1 is representative, and reads:

> *1. A method comprising:*
> *obtaining fingerprint data from a file header associated with a file, the fingerprint data being associated with contents of the file;*
> *checking the integrity of the fingerprint data;*
> *if the check leaves doubt about the fingerprint data thus obtained, then recalculating fingerprint data from contents of the file; and*
> *transmitting the fingerprint data to a database.*

Dependent claims 2-7 further elaborate on this method. Claim 2, for example, specifies accessing a database record corresponding to the transmitted fingerprint data, and returning associated information to a computer device from which the fingerprint data was transmitted.

---

6 *See, e.g.,* published specification US 2002/0032864, para. 30.
7 *Ibid.*

Claim 3 specifies that the file contents comprise audio. Claim 4 requires checking integrity of the fingerprint data by checking a digital signature.

Claim 5 specifies that the checking includes decrypting data from the header, and authenticating the decrypted data. Claim 6 further refines the method of claim 5 by requiring application of an inverse modification to the fingerprint in the header prior to decrypting. Claim 7 is like claim 6, but depends from claim 1.

VI. GROUNDS OF REJECTION

Claims 1-14 stand rejected under § 103 over McAuliffe (5,838,790) in view of Iwamura (6,425,081).

VII. ARGUMENT

1. Discussion of McAuliffe; Claim 1

McAuliffe discloses a system to assure that advertisements downloaded to a user's computer for later off-line display (e.g., in the Juno email program) are, in fact, correctly downloaded and displayed. The user's computer tracks which advertisements are presented to the user - and when (in an "advertisement statistics file" written on the user's hard disk), and the advertisers are billed accordingly. The McAuliffe system checks whether downloaded advertisements are modified or deleted, so that advertisers won't be billed for advertising that is not presented as intended to users.

More particularly, when McAuliffe transmits an advertisement to a user's computer, it additionally sends along an encrypted "fingerprint" of the advertisement, allowing the user's computer to determine whether any tampering of the advertisement occurred in the transmission process.[9]

---

[8] *Ibid.*

When the user computer receives such an advertisement, it computes a fingerprint of the received advertisement, decrypts the encrypted fingerprint that was sent along with the advertisement, and compares the two for a match.[10] If the two don't match, a record is made in the advertisement statistics file, and the received advertisement is deleted.[11]

If the calculated and received/decrypted fingerprints match, McAuliffe stores the fingerprint in an encrypted file, and stores the authenticated advertisement in an advertisement directory on the user's hard disk.[12]

Thereafter, each time programming on the user's computer causes an advertisement to be displayed, it opens the encrypted file in which fingerprints are stored, and compares the stored fingerprint for the subject ad with a fingerprint newly computed from the ad.[13]

If the stored and calculated fingerprints do not match, McAuliffe does not proceed to display the ad, but instead stores an error message in the advertisement statistics file on the user's hard disk noting the failed authentication.[14]

The Final Rejection is premised on erroneous understanding of McAuliffe. For example, the Action states:

> *Claim 1: McAuliffe's patent teaches obtaining and checking the integrity of the fingerprint data in (col. 8, lines 7-15).* [15]

Contrary to this premise, McAuliffe does *not* check the integrity of fingerprint data.

The cited excerpt (col. 8, lines 7-15) teaches checking integrity *of the advertisement.*

McAuliffe checks the integrity of the advertisement by checking for expected correspondence between the advertisement and associated fingerprint data The advertisement may be suspect. The fingerprint data is not. McAuliffe's states that his system is based on

---

9 McAuliffe, col. 3, lines 49-65; col. 4, lines 8-12; Fig. 1, box 106.
10 McAuliffe, col. 7, lines 15-25.
11 McAuliffe, col. 7, lines 15-33.
12 McAuliffe, col. 7, lines 34-38.
13 McAuliffe, col. 7, lines 48-53; col. 8, lines 7-17.
14 McAuliffe, col. 8, lines 11-15.
15 Final Rejection, April 20, 2005, page 2, lines 12-13.

fingerprints "*known to be secure.*"[16]

Thus, if the stored and calculated fingerprint data don't match, this indicates corruption or alteration of the advertisement file.[17] Nothing is learned about the integrity of the fingerprint.

Further, applicants' claim 1 says "if the check leaves doubt about the fingerprint data..." Again, McAuliffe does not suggest any possible "doubt" about the fingerprint data.

Moreover, if the check leaves doubt about the fingerprint data obtained from the file header, claim 1 further requires "*recalculating fingerprint data from contents of the file.*" In McAuliffe's system, his client program *always* calculates a fingerprint from the received data.[18] It is this calculated fingerprint that is compared against the fingerprint transmitted from the server to determine if the advertisement has been tampered with.[19] Calculating the fingerprint is part of the process in McAuliffe that *gives rise* to the doubt – not an action that is taken after doubt has arisen.

Still further, applicants' claim 1 calls for "transmitting the fingerprint data to a database [if the check leaves doubt about the fingerprint data]." On this act, too, McAuliffe is silent. (The Examiner cites col. 8, lines 12-17 for such teaching, but this excerpt instead teaches storing an error message in the advertisement statistics file, and computing a fingerprint of the advertisement statistics file.)

In addition to the foregoing shortcomings, the Action proposes combing McAuliffe with Iwamura (which teaches storing hash data in a file header), offering the inadequate rationale:

> *It would have been obvious to person of ordinary skill in the art at the time invention was made to embed or obtain fingerprint data from a file header, as taught in*

---

16 McAuliffe, col. 3, line 58.

17 McAuliffe, col. 7, lines 30-31; col. 8, lines 18-20.

18 McAuliffe, col. 8, lines 8-9 ("*...the client program calculates the fingerprint of the retrieved advertisement file A...*").

19 McAuliffe, col. 8, lines 10-11 ("*...and compares this [calculated fingerprint] with the fingerprint F obtained from the encrypted file...*").

Iwamura with data embedding method disclosed in McAuliffe because when fingerprint data is embedded in a image/data, it distorts original data and error tends to occur by fingerprint data. Therefore, embedding fingerprint data in a non-display field such as header file is highly desirable. Further, by separating fingerprint data from original data, fingerprint data is protected and well secured and allows for efficient data transmission with minimal interference.

This rationale is not understood. It references a "data embedding method disclosed in McAuliffe" when no data embedding appears to be taught. It urges "separating fingerprint data from original data" – when such separation is already afforded by McAuliffe. It references distortion of original data, and error that "tends to occur by fingerprint data," when no such distortion or error seems contemplated by McAuliffe.

Since the McAuliffe reference fails to teach various of the acts for which the Action cites it, a *prima facie* showing under Section 103 has not been established. Because the art fails to teach that for which it has been cited, the art cannot be combined to yield the combination of claim 1. Moreover, the proposed combination with Iwamura also fails for not being suggested by the art.

Reversal is required.

2. Claim 2

Claim 2 depends from claim 1 and is similarly allowable. Moreover, claim 2 is patentable independently. The claim reads:

2. The method of claim 1 that includes:
accessing a database record corresponding to the transmitted fingerprint data, to obtain associated information; and
returning at least some of said associated information to a computer device from which the fingerprint data was transmitted.

The Action cites McAuliffe at col. 9, lines 24-37 for this teaching.

Col. 9, lines 24-37, discloses how McAuliffe's updates his customer information database to reflect any failed transmission of the advertisement file.

This passage does not teach or suggest accessing a database record *corresponding to the transmitted fingerprint data.*

Again, the art does not teach that for which it has been cited. Again, reversal is required.

3. Claim 3

Claim 3 stands or falls with claim 1, from which it depends.

4. Claim 4

Claim 4 depends from claim 1 and is similarly allowable. Moreover, claim 4 is patentable independently. The claim reads:

> *4. The method of claim 1 in which checking includes checking a digital signature.*

The Action acknowledges that McAuliffe does not teach this limitation.[20]

Iwamura is cited to fill this gap, with the Action stating:

> *It would have been obvious to person of ordinary skill in the art at the time invention was made to employ a digital signature as taught in Iwamura with fingerprint checking disclosed in McAuliffe in order to assure the data recipient that the original source is authentic and legitimate which allows secure and reliable way to authenticate its documents and its source. Further, digital signature protects against repeated usage, forged document and repudiation.*[21]

Applicants respectfully submit that this combination is impermissibly premised on hindsight.

First, Iwamura is drawn from different art; it does not concern downloading of advertisements for offline display – the field to which McAuliffe is directed. (Iwamura concerns digital watermarking.)

---

20 Final Rejection, April 20, 2005, page 3, line 5.

21 Final Rejection, April 20, 2005, page 3, lines 6-11.

Moreover, in McAuliffe, if an artisan sought "to assure the data recipient that the original source is authentic and legitimate," the artisan would have focused on the received data of concern, i.e., the *advertisement* data. (Authenticity of McAuliffe's *fingerprint* data isn't an end he aims to achieve, rather his use of a fingerprint data is simply a means he employs to achieve his end aim - authenticating the *advertisement* data.) Thus, if any application of digital signature technology were considered by an artisan, same would have been applied to the advertisement, not the fingerprint.

Again, the rejection has failed to meet the *prima facie* burden, and must be reversed.

5. Claim 5

Claim 5 depends from claim 1 and is similarly allowable. Moreover, claim 5 is patentable independently. The claim reads:

> *5. The method of claim 1 in which the checking includes decrypting fingerprint data from the header and authenticating the decrypted data.*

The Action cites col. 7, lines 15-25, for this claim limitation.[22]

The Action is correct that the cited passage of McAuliffe teaches decrypting fingerprint data. However, this passage – as elsewhere - fails to teach that such fingerprint data is decrypted *from the header*. Moreover, McAuliffe fails to teach *authenticating* the decrypted fingerprint data.

Again, the art fails to teach claim limitations for which it cited, and the rejection must thus be reversed.

6. Claim 6

Claim 6 depends from claim 5 and is similarly allowable. Moreover, claim 6 is patentable independently. The claim reads:

---

[22] Final Rejection, April 20, 2005, page 3, lines 12-13.

6. The method of claim 5 that includes applying an inverse modification to the fingerprint in the header prior to said decrypting.[23]

The Action acknowledges that none of the art teaches this limitation.[24]

To redress this shortcoming, the Action relies on "Official Notice," stating:

Official notice is taken that applying an inverse modification to the fingerprint in the header prior to decrypting is well known in the art. One of ordinary skill in the art would haven motivated to employ inverse modification or also known as Modified Discrete Cosine Transform/inverse Modified Discrete Cosine Transform in order to reduce computation steps to produce output data. Inverse transformation allows less latency between the end of decoding and the start of the data output operation therefore it enhances speed of data processing. Since inverse modification is applied prior to decrypting, it allows decryption process to run faster thus minimizing data error rate.

While this logic is remarkable in numerous respects (*e.g.*, asserting that "applying an inverse modification to the fingerprint in the header prior to decrypting" is well known in the art), this rationale does not suggest the arrangement of claim 6.

Again, *prima facie* obviousness has not been established, and reversal is required.

7. Claim 7

Claim 7 stands or falls with claim 6.

8. Claim 8

Claim 8 is an independent claim, structurally modeled after claim 1, but dealing with watermark technology:

---

[23] Support for this limitation is found, e.g., in paragraph 37 of applicants' published specification US 2002/0032864.

[24] Final Rejection, April 20, 2005, page 3, lines 14-15.

8. A method comprising:
obtaining watermark data from a file header associated with a file, the watermark data being associated with contents of the file;
checking the integrity of the watermark data;
if the check leaves doubt about the watermark data thus obtained, then detecting watermark data from contents of the file; and
transmitting the watermark data to a database.

It will be recognized that this method allows a file watermark to be quickly discerned (*i.e.*, by reading same from the header), and allows for an alternative way to obtain the watermark (*i.e.*, by detecting from file contents) if integrity of the watermark data obtained from the header is dubious.

Again, the Final Rejection of this claim has several failures.

For example, while the Action correctly notes that McAuliffe has no disclosure concerning watermark data, it wrongly cites Iwamura as teaching the missing claim limitations.[25] (It will be recognized that each clause of the claim – excerpt the three word preamble – refers to "watermark data.") Iwamura fails to teach all these limitations.

For example, Iwamura does not teach "obtaining watermark data from a file header." Rather, in the passage cited by the Examiner (col. 21, lines 41-53),[26] Iwamura's file header is said to convey a *hash value*. This hash value is not Iwamura's watermark data. Conveying watermark data in the file header, as required by claim 8, is not taught or suggested by Iwamura.

Likewise, the claim calls for detecting watermark data from the file contents ***if*** integrity of watermark data in the header is checked, and found to be in doubt. Iwamura teaches a different arrangement, in which the "*first*" action in the verification process is detecting watermark data. (He states the first action is decoding the watermarked image to extract user information U watermarked therein.[27]) Iwamura does not teach detecting watermark data from the file contents only if a check of information in the header leaves doubt.

Still further, Iwamura does not teach "checking the integrity of the watermark data."

---

25 Final Rejection, page 4, lines 4-20.
26 Final Rejection, page 4, line 14.
27 *See, e.g.*, Iwamura at col. 18, lines 52-53, giving the "First" action (under the "Verification" process) as extraction of the user info U from the watermarked image G_W'. (That G_W' is the watermarked image is shown, *e.g.*,

The Action seems to rely on McAuliffe for this "checking" limitation. The Action again cites the excerpt at col. 8, lines 7-15 that deals with authenticating McAuliffe's advertisement, and terms it "checking the integrity of the data."[28] However, this overlooks the fact that the claim limitation requires "checking the integrity of the watermark data" – a limitation not met by checking advertisement data.

The Action's treatment of McAuliffe is further flawed. For example, the Action states "*McAuliffe discloses if the check leaves doubt about the data obtained, then recalculating fingerprint data from contents of the file and transmitting the data to a database.*"[29] As discussed above in connection with claim 1, McAuliffe contains no such disclosures. (Moreover, claim 8 does not concern "fingerprint data.")

Finally, as before, the rationale urging the selective modification and combination of McAuliffe and Iwamura is flawed – drawing from disparate arts, and falling short of compelling analysis:

> *It would have been obvious to person of ordinary skill in the art at the time invention was made to use watermark data, as taught in Iwamura with data embedding method displaced in McAuliffe because watermark data is preserved if the data is manipulated by processes such as compression or cropping. One of ordinary skill in the art would have been motivated to use watermark because watermark data is hardly visible and/or audible, it is difficult for backers to remove by unauthorized means yet it is easily detectable through an authorized or intended procedure. McAuliffe does not specifically disclose obtaining watermark data from a file header associated with a file. Iwamura's patent discloses in the verification process where data or hash value is embedded and obtained from a header in (col. 21, lines 41-53). It would have been obvious to person of ordinary skill in the art at the time invention was made to embed or obtain data from a file header, as taught in Iwamura with data embedding method disclosed in McAuliffe because when data is embedded in a image/data, it distorts original data and error tends to occur by this event. Therefor, embedding watermark data in a non-display field such as header file is highly desirable. Further, by separating watermark data from original data, watermark data is protected and well secured and allows for efficient data transmission with minimal interference.*[30]

---

at col. 18, lines 26-27.)

[28] Final Rejection, page 4, lines 1-2.

[29] Final Rejection, page 4, lines 2-3.

[30] Final Rejection, page 4, lines 5-20.

Concerning this purported rationale, it appears watermark's resilience to data manipulation makes it exactly what McAuliffe would avoid, rather than adopt. After all, McAuliffe's aim is to detect tampering. Since watermark data is preserved despite many forms of tampering, it appears McAuliffe's aim would be frustrated by adoption of such technology.

More fundamentally, neither McAuliffe nor Iwamura recognized the problem addressed by the present inventors. The rationale, above, does not address the problem solved by the present inventors. Absent such recognition, an artisan would not have found obvious the method of claim 8.

Again, the rejection is multiply-flawed, and reversal is required.

9. Claim 9

Claim 9 depends from claim 8 and is similarly allowable. Moreover, claim 9 is patentable independently. The claim reads:

> *9. The method of claim 8 that includes:*
> *accessing a database record corresponding to the transmitted watermark data, to obtain associated information; and*
> *returning at least some of said associated information to a computer device from which the watermark data was transmitted.*

The Action cites McAuliffe at col. 9, lines 24-37 for this teaching.

Col. 9, lines 24-37, discloses how McAuliffe's updates his customer information database to reflect any failed transmission of the advertisement file.

This passage does not teach or suggest accessing a database record *corresponding to the transmitted watermark data*. Nor does Iwamura cure such deficiency.

Again, the art does not teach that for which it has been cited. Again, reversal is required.

10. Claim 10

Claim 10 stands or falls with claim 8, from which it depends.

11. Claim 11

Claim 11 depends from claim 8 and is similarly allowable. Moreover, claim 11 is patentable independently. The claim reads:

> *11. The method of claim 8 in which checking includes checking a digital signature.*

The Action acknowledges that McAuliffe does not teach this limitation.[31] Iwamura is cited to fill this gap, with the Action stating:

> *It would have been obvious to person of ordinary skill in the art at the time invention was made to employ a digital signature as taught in Iwamura with fingerprint checking disclosed in McAuliffe in order to assure the data recipient that the original source is authentic and legitimate which allows secure and reliable way to authenticate its documents and its source. Further, digital signature protects against repeated usage, forged document and repudiation.*[32]

Again, applicants respectfully submit that this combination is impermissibly premised on hindsight.

First, Iwamura is drawn from different art; it does not concern downloading of advertisements for offline display – the field to which McAuliffe is directed. (Iwamura concerns digital watermarking.)

Moreover, in McAuliffe, if an artisan sought "to assure the data recipient that the original source is authentic and legitimate," the artisan would have focused on the received data of concern, i.e., the *advertisement* data. (Authenticity of McAuliffe's *fingerprint* data isn't an end he aims to achieve, rather his use of a fingerprint data is simply a means he employs to achieve his end aim - authenticating the *advertisement* data.) Thus, if any application of digital signature technology were considered by an artisan, same would have been applied to the advertisement,

---

31 Final Rejection, April 20, 2005, page 3, line 5.
32 Final Rejection, April 20, 2005, page 3, lines 6-11.

not McAuliffe's fingerprint. (Again, the Office seems to have given no consideration to the "watermark" requirement of the claim – citing instead "fingerprint" language from McAuliffe.)

Again, the rejection has failed to meet the *prima facie* burden, and must be reversed.

12. Claim 12

Claim 12 depends from claim 8 and is similarly allowable. Moreover, claim 12 is patentable independently. The claim reads:

> *12. The method of claim 5 in which the checking includes decrypting watermark data from the header and authenticating the decrypted data.*

The Action cites McAuliffe at col. 7, lines 15-25, for this claim limitation.[33]

That passage, however, relates to decrypting *fingerprint* data. McAuliffe has no disclosure concerning watermark data. And the passage has no teaching concerning "authenticating" the decrypted data.

Iwamura is again cited to fill the "watermark" gap. But it does nothing to fill the "authenticating" gap. (And, as before, the rationale for combining Iwamura with McAuliffe fails on multiple grounds.)

Again, the art fails to teach claim limitations for which it cited, and the rejection must thus be reversed.

13. Claim 13

Claim 13 depends from claim 12 and is similarly allowable. Moreover, claim 13 is patentable independently. The claim reads:

> *13. The method of claim 12 that includes applying an inverse modification to the watermark in the header prior to said decrypting.*

---

[33] Final Rejection, April 20, 2005, page 3, lines 12-13.

The Action acknowledges that none of the art teaches this limitation.[34]

To redress this shortcoming, the Action relies on "Official Notice," again stating:

> *Official notice is taken that applying an inverse modification to the fingerprint in the header prior to decrypting is well known in the art. One of ordinary skill in the art would haven motivated to employ inverse modification or also known as Modified Discrete Cosine Transform/inverse Modified Discrete Cosine Transform in order to reduce computation steps to produce output data. Inverse transformation allows less latency between the end of decoding and the start of the data output operation therefore it enhances speed of data processing. Since inverse modification is applied prior to decrypting, it allows decryption process to run faster thus minimizing data error rate.*

Again, this rationale falls short of the Office's burden to show recognition of the problem faced by applicants, nor an obvious realization that the problem could be addressed by borrowing teachings from other sources.

Again, *prima facie* obviousness has not been established, and reversal is required.

14. Claim 14

Claim 14 stands or falls with claim 13.

---

[34] Final Rejection, April 20, 2005, page 3, lines 14-15.

VIII. CONCLUSION

None of the rejections meets the *prima facie* burden. The cited art does not teach the limitations alleged. The claimed arrangements could not result from combinations of such art. The Final Rejection proposes combinations that are not suggested by the art, and that could not be implemented from the references' teachings even with hindsight.

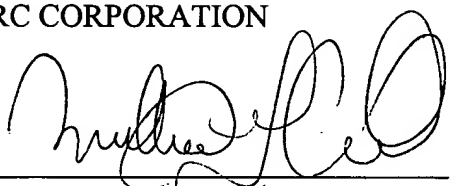
Accordingly, the Board is requested to rule that claims 1-14 should be passed to issuance.

Respectfully submitted,

Date: September 26, 2005

DIGIMARC CORPORATION

CUSTOMER NUMBER 23735



By_____

William Y. Conwell
Registration No. 31,943

Phone: 503-469-4800
FAX 503-469-4777

APPENDIX A

PENDING CLAIMS

1. A method comprising:

obtaining fingerprint data from a file header associated with a file, the fingerprint data being associated with contents of the file;

checking the integrity of the fingerprint data;

if the check leaves doubt about the fingerprint data thus obtained, then recalculating fingerprint data from contents of the file; and

transmitting the fingerprint data to a database.

2. The method of claim 1 that includes:

accessing a database record corresponding to the transmitted fingerprint data, to obtain associated information; and

returning at least some of said associated information to a computer device from which the fingerprint data was transmitted.

3. The method of claim 1 in which the file contents comprise audio.

4. The method of claim 1 in which checking includes checking a digital signature.

5. The method of claim 1 in which the checking includes decrypting fingerprint data from the header and authenticating the decrypted data.

6. The method of claim 5 that includes applying an inverse modification to the fingerprint in the header prior to said decrypting.

7. The method of claim 1 that includes applying an inverse modification to the fingerprint in the header.

8. A method comprising:

obtaining watermark data from a file header associated with a file, the watermark data being associated with contents of the file;

checking the integrity of the watermark data;

if the check leaves doubt about the watermark data thus obtained, then detecting watermark data from contents of the file; and

transmitting the watermark data to a database.

9. The method of claim 8 that includes:

accessing a database record corresponding to the transmitted watermark data, to obtain associated information; and

returning at least some of said associated information to a computer device from which the watermark data was transmitted.

10. The method of claim 8 in which the file contents comprise audio.

11. The method of claim 8 in which checking includes checking a digital signature.

12. The method of claim 8 in which the checking includes decrypting watermark data from the header and authenticating the decrypted data.

13. The method of claim 12 that includes applying an inverse modification to the watermark in the header prior to said decrypting.

14. The method of claim 12 that includes applying an inverse modification to the watermark in the header.